



# أكتوبر/ تشرين الأول 2024 شهر الوعي بالأمن السيبراني احم نفسك!

## 1. كن على حذر من الرسائل الإلكترونية الاحتيالية

الاحتيال هو عندما يحاول المجرمون الافتراضيون سرقة المعلومات عبر عناوين إلكترونية زائفة. هم يتظاهرون بكونهم أشخاص آخرين ويريدون منك النقر على روابط خطيرة. إذا بدت رسالة إلكترونية غريبة، كن على حذر، وتحقق من مرسلها وما إذا كان العنوان الإلكتروني يتوافق مع معلومات الشخص الذي يدعي أنه صاحبها.

## 2. استخدم المصادقة متعددة العوامل (MFA)

احصل على طبقة أخرى من الحماية ضد القرصنة عندما تسجل دخول إلى حساب (MFA). وذلك عبارة عن نص فيه رمز سري تنتهي صلاحيته بعد استخدامه لمرة واحدة.

## 3. استخدم كلمات مرور أو عبارات مرور قوية

لا تستخدم نفس كلمة السر في كل مكان! استخدم الأحرف، والأرقام، والرموز. بقدر ما تكون كلمة السر أو عبارات المرور طويلة بقدر ما تكون أفضل.

## 4. واصل تحديث البرمجيات الخاصة بك

فهذا يقلل من خطر العدوى من البرمجيات التي يقوم القرصنة بتنزيلها والتي يمكنها سرقة معلوماتك أو نشر الفيروسات في جهاز الكمبيوتر الخاص بك.

## 5. كن ذكياً وآمناً في مواقع التواصل الاجتماعي!

يمكن أن يتم استخدام مشاركة المعلومات الشخصية مثل تاريخ ميلادك الكامل، أو عنوان البيت، أو موقعك، لسرقة الهوية أو للتنمر.

## 6. احم نفسك – استخدم شبكة واي فاي آمنة

إن مواقع شبكات الإنترنت العامة غير محمية. قد يتمكن شخص ما من رؤية ما تقوم به على الإنترنت بما في ذلك الدخول إلى بريدك الإلكتروني وحساباتك المصرفية.

## 7. كن على حذر من عمليات الاحتيال المنتجة بالذكاء الاصطناعي

يستخدم المجرمون السيبرانيون الذكاء الاصطناعي المتقدم لتشكيل صور واقعية، ونصوص، وأصوات، وفيديوهات. وهذا يجعل التنبيه الاحتيال وعمليات الغش الأخرى أكثر صعوبة. كن يقظاً وأعد الفحص (مثلاً تحقق من المصدر، ابحث عن العلامات التحذيرية الخاصة بالذكاء الاصطناعي و"الأدوات" مثل اللغة الاستعجالية، أو الأصوات غير الطبيعية، أو الصور المحرفة قليلاً، إلخ) قبل أن تثق بأي تواصل غير متوقع.